PRIMITIVE IRREDUCIBLE LINEAR GROUPS

a thesis submitted for the degree of
Master of Science at the
Australian National University

by William Hulme Wilson

1972

Supervised by P.J. Cossey and M.F. Newman

Contents.

Summary.

This thesis examines several unrelated aspects of primitive irreducible linear groups. The initial section is introductory. In chapter 1, it is shown that the Fitting subgroup of a certain subgroup of finite index in a primitive irreducible linear group is always nilpotent of class at most two. In the next chapter, results of D.A. Suprunenko on the structure of maximal soluble irreducible and maximal soluble primitive irreducible linear groups are extended, as much as possible, to the nonmaximal, nonsoluble case. In chapter 3, it is shown that under certain conditions on the field, maximal soluble primitive irreducible linear groups of degree 2 are split extensions of their Fitting subgroup by the symmetric group of degree 3. In the final section, a result of Suprunenko on tensor product decompositions of maximal soluble primitive irreducible linear groups is examined from another angle, again without assuming that the group is maximal soluble.

Acknowledgements.

Some of this work arose from problems which cropped up in a project on soluble linear groups done in my final undergraduate year. This project, and the first six months of the M.Sc. work, were supervised by Dr M.F. Newman. The rest of the work was supervised by Dr P.J. Cossey. To both, I am sincerely grateful. Their contributions were of both the strategic and tactical variety: a partial record of the tactical assistance appears in the text.

Apart from these reservations, and except where otherwise stated, this work is my own.

My five years at the Australian National University were supported financially by a National Undergaduate Scholarship (1966-1969) and an A.N.U. Master's Degree Scholarship (1970). I take this opportunity to record my gratitude to the University for this assistance.

..... W. H. Wilson

The statement below is inserted to explain an unproven assertion in chapter 3. The fact that it was unproven was pointed out to me by the examiners.

The conclusion (at the bottom of page 34) that $G/A \cong S_3 \cong Sp(2,2)$ is unwarranted at that stage. However, we can show that the matrices $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ in $Sp(2,2)$ are induced by matrices g and h in $GL(2,P)$ acting on A/F via

$aF \mapsto [a,g]F$ and $aF \mapsto [a,h]F$;

the equation-solving on page 39 explicitly produces such matrices g and h. Hence $N_{GL(2,P)}(A)/A$ has elements of order 2 and 3 so has order at least 6, but is embedded in $Sp(2,2)$ so has order exactly 6. It follows that $N_{GL(2,P)}(A)$ is soluble, so by the maximality of G, $N_{GL(2,P)}(A) = G$. So $G/A \cong S_3$.

0. Introduction: Definitions, Notation, Basic Results.

The following is a list of non-standard notation that will be used, most other notation will agree with that used in Huppert, 1967.

$[X]$	...	Linear hull of X - see definition 0.2
P_n	...	full ring of nxn matrices over field P
$GL(n,P)$	...	group of units of P_n
$GF(q)$	...	Galois field of order q
I_n	...	nxn identity matrix
P^x	...	multiplicative group of field P
$\dim_P K$	...	dimension or degree of field K over P
$C_G(V)$	...	if V is a vector space - $\{g \in G: \forall v \in V, vg = v\}$
$N_G(V)$	...	if V is a vector space - $\{g \in G: Vg = V\}$
$Z_n(G)$	...	n^{th} term of upper central series of group G
$A \curlyvee_Z B$	...	central product of groups A,B amalgamating subgroup Z - see Huppert 1967 for a rigorous definition (page 49)
//	...	denotes "end of proof" or "proof omitted"

0.1: We assume that the reader is familiar with the notions of linear group, module, submodule, faithful module, irreducible module. In this section the notions of irreducible linear group and primitive linear group will be defined, and the following questions asked and partly answered:

(i) how do subgroups of primitive/irreducible groups behave?

(ii) how do primitive/irreducible groups react to field extensions?

(iii) how do tensor products of primitive/irreducible groups behave?

0.2: Definition. For $X \subseteq P_n$, the P-linear hull $[X]$ of X is the smallest P-subalgebra of P_n containing X.

0.3: Definition. Let $G \leqslant GL(n,P)$ be a linear group. We say that G is irreducible, reducible, or completely reducible according as $P^{(n)}$, the n-dimensional row vector space, is irreducible, reducible, or completely reducible as $[G]$-module under the natural action.

0.4: Definition. Let $P^{(n)} = Q_1 \oplus \ldots \oplus Q_r$ be a vector space direct sum decomposition of $P^{(n)}$ with $r \neq 1$, and let $G \leqslant GL(n,P)$ be a linear group acting on $P^{(n)}$ in such a way that each $g \in G$ permutes the subspaces Q_i. Then $\{Q_i\}$ is called a system of imprimitivity for G, and G is said to be an imprimitive subgroup of GL(n,P). If no such decomposition exists, G and $P^{(n)}$ are called a primitive group and primitive G-module respectively. If G is imprimitive, it is not hard to see that there exists a minimal or complete system of imprimitivity, that is, one for which r (the number of spaces Q_i) is maximal. It is also clear that an irreducible group permutes any system of imprimitivity transitively.

The next theorem is the answer to question (i) for irreducible and primitive irreducible groups. Since it is well-known, we omit the proof (see Huppert 1967, p565, for example). Succeeding results are consequences of Clifford's theorem which turn out to be useful later on.

0.5: Clifford's Theorem. Let G be an irreducible subgroup of GL(n,P) and H a normal subgroup of G. Then $P^{(n)}$ is completely reducible into [H]-modules of equal P-dimension. If $W_1, \ldots, W_r$ are the homogeneous components of $P^{(n)}$ as [H]-module, then $\{W_1, \ldots, W_r\}$ is a system of imprimitivity for G. Thus if G is also primitive, then $P^{(n)}$ is completely reducible into [H]-isomorphic [H]-modules. //

0.6: Corollary.[1] Let G, H be as in Clifford's theorem, with G primitive. Then:

(i) H has a faithful irreducible representation over P, of degree dividing n.

(ii) [H] is a simple algebra over P, and so is isomorphic to a full matrix algebra over a skewfield. Consequently, if H is Abelian, [H] is a field K extending P, such that $\dim_P K$ divides n, and $K^{(r)} = P^{(n)}$, where $r = n/\dim_P K$. Further, $C_G(H)$ is embedded in GL(r,K).

Proof: (i) By (0.5), $P^{(n)} = Q_1 \oplus \ldots \oplus Q_r$, where the Q_i are isomorphic irreducible [H]-modules of P-dimension n/r. We will prove that [H] acts faithfully on Q_1. Suppose that $h \in [H]$ induces the identity transformation on Q_1. Every $q \in P^{(n)}$ can be written (uniquely) in the form $q = q_1 + \ldots + q_r$, with $q_i \in Q_i$, and the primitivity of G guarantees that there exist [H]-isomorphisms $\Theta_i: Q_1 \longrightarrow Q_i$. So

$$q_i \Theta_i^{-1} h = q_i \Theta_i^{-1}, \quad \text{but on the other hand}$$

1. Taken from various parts of Suprunenko, 1963.

$$q_i\theta_i^{-1}h = q_ih\theta_i^{-1} ,$$

so $q_ih = q_i$ and thus

$$qh = (q_1+\ldots+q_r)h = q_1h+\ldots+q_rh = q_1+\ldots+q_r = q.$$

So h induces the identity transformation on all of $P^{(n)}$, that is, $h = I_n$.

(ii) By Huppert 1967, page 469, every algebra with a faithful irreducible module is simple, and by the well-known Wedderburn's theorem (Huppert 1967, page 472), $[H]$ is thus isomorphic to a full kxk matrix ring over some skewfield. It is not hard to see that if H is Abelian, the skew field has to be commutative and $k = 1$. Thus $P^{(n)} = q_1K \oplus \ldots \oplus q_rK$ for any choice of $q_i \in Q_i$, $q_i \neq 0$, since all the Q_i are K-irreducible. That is, $P^{(n)} = K^{(r)}$ and $\dim_P K = n/r$.

Finally, $C_G(H) = C_G([H])$, and so each $c \in C_G(H)$ is a K-linear transformation of $K^{(r)}$. //

0.7: Corollary. (Compare Suprunenko 1963, page 58). If G is an irreducible subgroup of GL(n,P) and Z is any central subgroup of G, then G can be embedded as an irreducible subgroup of GL(r,K), where K is an extension field of P of degree n/r, and $Z \leq K^x.I_r$. If G is $P^{(n)}$-primitive then it is $K^{(r)}$-primitive too.

Proof: The linear hull of Z is a commutative algebra of finite dimension over P. Also $[Z] \subseteq C_{P_n}(G)$, which is a skewfield by Schur's lemma (Huppert 1967, page 471). So $[Z]$ has no zero divisors and thus is semisimple. As a

commutative semisimple algebra without zero divisors, [Z] is a field (see Herstein 1968, p54). Call this field K. The rest follows from (0.5) and arguments similar to those of (0.6). //

(0.7) and (0.8) shed some light on the question: when do linear groups remain irreducible and/or primitive after the field has been extended?

0.8: Proposition. Let G be an irreducible subgroup of GL(n,P). Then there exists a finite extension field K of P, and a subgroup H of GL(r,K), where $r = n/\dim_P K$, such that H is isomorphic to G and also absolutely irreducible. (Taken from notes on linear groups by B.A.F. Wehrfritz.)

Proof: By Schur's lemma, $D = C_{P_n}(G)$ is a division ring. By Herstein 1968, p105, we can choose a maximal subfield K of D with the following properties: K contains $P^x.I_n$; $K = C_D(K)$; $n = \dim_P K.m$ for some integer m. $P^{(n)}$ is naturally a vector space over K, and since K-linear maps are a fortiori P-linear, there exists a K-algebra isomorphism $\phi: C_{P_n}(K) \longrightarrow K_m$.

Since $K \subseteq C_{P_n}(G)$, $G \subseteq C_{P_n}(K)$, so we can set $H = G\phi$. Now $C_{P_n}(K) \cap C_{P_n}(G) = C_{P_n}(K) \cap D = C_D(K) = K$. That H is absolutely irreducible now follows from Curtis and Reiner, 1962, (29.13). //

Note that if G is primitive, then so is H.

It is not hard to see that if a tensor product of groups is irreducible or primitive, then the factors are, too. It is well-known that if the factors are absolutely irreducible, then the tensor product is, too. With regard to field extensions, we have 0.7 and 0.8, but note that an arbitrary field extension can destroy both primitivity and irreducibility.

1. Fitting Subgroups of Primitive Irreducible Linear Groups.

In this chapter, we examine Fitting subgroups in primitive irreducible linear groups. In the case of a linear group over an algebraically closed field, it is known (see Suprunenko 1963, p60) that irreducible nilpotent linear groups are never primitive: this fact lends interest to the discussion. In fact we shall prove that primitive irreducible groups can be nilpotent in the case of certain finite fields. The first such example was shown to me by M.F. Newman.

1.1: Definition. The Hirsch-Plotkin radical, $\rho(G)$, of a group G, is defined to be the subgroup generated by all the locally nilpotent normal subgroups of G. The Fitting subgroup Fit(G) of G is defined to be the subgroup of G generated by all the nilpotent normal subgroups of G. Clearly $Fit(G) \leq \rho(G)$. It is known that the Fitting subgroup of a finite group is nilpotent, and that the Hirsch-Plotkin radical of any group is the unique maximal locally nilpotent normal subgroup of that group.

1.2: Lemma (P.J. Cossey). Let G be a nilpotent group such that $Z(Z_2(G)) = Z(G)$. Then G is of class at most 2.

Proof: Let c be the class of G. By Huppert 1967, III.2.11b, $K_{c-1}(G/Z) \leq Z(G/Z) = Z_2/Z$, where K_{c-1} denotes the $c-1^{st}$ term of the lower central series. Hence, either $c = 2$, or there exists a commutator $[x_1, \ldots, x_{c-1}] \in Z_2 \cap (G' \setminus Z)$. By Huppert 1967, III.2.11c, G' commutes with Z_2, so $G' \leq C_G(Z_2)$. Therefore $Z_2 \cap G' \leq Z(Z_2) = Z$, by hypothesis.

In particular, $[x_1, \ldots, x_{c-1}] \in Z$, contradicting the previous statement that $[x_1, \ldots, x_{c-1}] \in Z_2 \cap (G' \setminus Z)$. //

1.3: Theorem. Let G be a primitive irreducible subgroup of GL(n,P), F a maximal Abelian normal subgroup of G, and set $V = C_G(F)$. Then Fit(V) is nilpotent of class at most 2.

Proof: (i) We first establish that G/V is finite, by embedding it in the Galois group of a finite field extension. I claim that the P-linear hull of F is a field extending P: this is just what 0.6(ii) says. Call the field K. Clearly G normalises K, so induces automorphisms of K fixing P. The kernel of this indicated map from G to Gal(K;P) is $C_G(F) = V$. Hence G/V is finite by Adamson 1964, theorem 14.2.

(ii) Next we show that a normal nilpotent subgroup N of G, if contained in V, is of class at most 2.

Clearly $F = Z(V)$. By 0.6(i), $Z_2(N)$ has a faithful irreducible representation over P of some degree dividing n. It follows from 0.7 that $Z(Z_2) = Z_2 \cap K^x.I$, where K is an extension field of P of finite degree, and I is an identity matrix of suitable size. By the remark at the beginning of this paragraph, we can assume without loss of generality that $F \leqslant N$ and so $F \leqslant Z(N)$. It follows that $F \leqslant Z(Z_2(N))$, and so, by the maximality of F, $F = Z(Z_2(N))$. Similarly $F = Z(N)$. Thus, by 1.2, N is of class at most 2.

(iii) Now let M be a normal nilpotent subgroup of

V such that $M \supseteq F$. Because V is of finite index in G, there are only finitely many groups conjugate to M in G. Clearly all of these are normal nilpotent subgroups of V, so by Fitting's theorem (Huppert 1967, III.4.1), the subgroup N that they generate is again nilpotent. Further, $N \trianglelefteq G$, $N \leqslant V$, so by the part above, N is of class at most 2, and hence so is M.

A standard Zorn's lemma argument using the fact that normal nilpotent subgroups of V are of class at most 2 shows that V has a maximal nilpotent normal subgroup, which is, of course, of class at most 2. Fitting's theorem guarantees its uniqueness, so this maximal nilpotent normal subgroup is the Fitting subgroup of V. //

A result will be proved in chapter 2 that will show that even the Hirsch-Plotkin radical of V is nilpotent of class at most 2, (so that in particular, $\varrho(V) = \mathrm{Fit}(V)$).

1.4: Corollary. If G is a primitive irreducible subgroup of GL(n,P) whose maximal Abelian normal subgroup is identical with its centre, then Fit(G) is nilpotent of class at most 2. In particular, this happens if P is algebraically closed.

Proof: The first part is obvious. By 0.6(ii), the linear hull of F is a field extending P and of finite dimension over P. If P is algebraically closed, this forces $[F] = P$, and so $F = P^{x}.I_n \cap G \leqslant Z(G)$. Here F is, of course, the maximal Abelian normal subgroup of G. //

We now proceed to construct counterexamples to the conjecture that Fit(G) is always of class at most 2.for primitive irreducible linear groups G. We do this by constructing high class nilpotent linear groups which are primitive and irreducible: in such a case, of course, Fit(G) = G.

1.5: Numerical lemma. If $k \geqslant 2$ and $m \geqslant 2$,

$$k^m - 1 > 3^{\frac{1}{3}m}(k - 1).$$

Proof: (a) For $k \geqslant 3$, it is easy to check that

$$k^{m-1} > 3^{\frac{1}{3}m} \quad \text{when } m \geqslant 2.$$

Hence $k^{m-1} + k^{m-2} + \ldots + k + 1 > 3^{\frac{1}{3}m}$ for $m \geqslant 2$,

so that $k^m - 1 > 3^{\frac{1}{3}m}(k - 1)$.

(b) For $k = 2$, we have to prove that $3^{\frac{1}{3}m} < 2^m - 1$. This is trivial for $m = 2$. Suppose inductively that

$$3^{\frac{1}{3}j} < 2^j - 1.$$

Then $3^{(j+1)/3} < (2^j - 1).3^{\frac{1}{3}} < 2(2^j - 1) < 2^{j+1} - 1$.

So by induction, (b) is proved. //

1.6: Proposition. Let p be a prime number. Then every Galois field $GF(p^r)$ has a faithful irreducible representation whose representation module is primitive, of degree r, over GF(p).

Proof: V.4.1 of Huppert 1967 guarantees a faithful irreducible representation. We examine the proof given there to obtain the degree. $GF(p^r)$ is a simple commutative GF(p)-algebra, so its only proper right ideal is (0). Huppert's proof says that $GF(p^r)/(0)$ is a faithful irreducible $GF(p^r)$-module. But

$\dim_{GF(p)} GF(p^r)/(0) = r$.

It remains to prove that $GF(p^r)/(0)$ is primitive. Let F denote the multiplicative group of $GF(p^r)$, and suppose that $\{Q_1,\ldots,Q_k\}$ is a system of imprimitivity for F. Set $N = \bigcap_{i=1}^{k} N_F(Q_i)$; it is easy to see that F/N acts as a permutation group on the Q_i. Pick a non-zero $q \in Q_1$: if $f \in N_F(Q_1)$ then there are at most $|Q_1 \setminus (0)|$ choices for qf and any choice completely determines the corresponding f. Now $|Q_1| = p^{r/k}$, so $|N| \leq |N_F(Q_1)| \leq p^{r/k} - 1$. Now an Abelian permutation group of degree k has order at most $3^{k/3}$ (Dixon 1967, page 418), so our assumption of imprimitivity leads to the conclusion that F has order at most $3^{k/3}.(p^{r/k} - 1)$. This contradicts the numerical lemma 1.5. //

By theorem 4.3.1 of Herstein 1968, for every $g \in Gal(GF(p^r);GF(p))$, there exists a matrix $C(g)$ in $GL(r,p)$ such that $C(g)$ induces by conjugation the automorphism g on the isomorphic copy of $GF(p^r)$ in $GL(r,p) \cup (0)$ described in 1.6. Hence $GF(p^r)^x$ split extended by the above Galois group is embedded as a primitive irreducible subgroup of $GL(r,p)$, because the mapping $g \mapsto C(g)$ is an isomorphism (by Herstein 1968, lemma 4.4.2).

To achieve the stated aims, it remains to prove that this split extension is sometimes nilpotent of class higher than 2. Let us denote our split extension by the symbol $G_{r.p}$ where the subscripts have the obvious meaning.

1.7: Theorem. $G_{r,p}$ is nilpotent of class j if $p^r - 1$ divides $(p - 1)^j$ but not $(p - 1)^{j-1}$. This is the case if r=2 and p is a Mersenne prime, that is, one of the form $p = 2^q - 1$. The class of $G_{2,2^q-1}$ is q + 1. The largest known Mersenne prime is,,I believe, $2^{11213} - 1$.

Proof: The Galois group of $GF(p^r)$ over GF(p) is cyclic of order r - let us suppose that the copy of the Galois group in $G_{r,p}$ is generated by a matrix y, and that the copy of $GF(p^r)^x$ is generated by a matrix f. Calculating, $[f,y] = f^{p-1}$; using this fact, it is not hard to check that $G_{r,p}$ is nilpotent of class j, where j is as in the statement of the theorem.

If r=2 and $p = 2^q - 1$, then we want to show that p + 1 divides $(p - 1)^q$ but not $(p - 1)^{q-1}$ - that is, that 2^q divides $(2^q - 2)^q$ but not $(2^q - 2)^{q-1}$. But this is clear. //

2. The Structure of Primitive and Imprimitive Irreducible Linear Groups.

The results in this section can often be used as tools to solve problems about linear groups in general. One reduces the given problem to one about irreducible linear groups, then to primitive irreducible linear groups. The main theorem of this section can then be used, giving information about the structure of primitive irreducible linear groups.

Examples of this process are to be found in Dixon 1967, 1968.

Most of the results of this section were proved, under the additional assumption that the groups in question are maximal soluble subgroups of GL(n,P), by D.A. Suprunenko, and are to be found in his book (Suprunenko 1963).

We begin by stating a well-known result (see Curtis and Reiner 1962, for example) which often enables the reduction to the irreducible case, mentioned above, to be made:

2.1: Theorem. If G is a reducible subgroup of GL(n,P), then there exists a matrix $x \in GL(n,P)$ such that for all $g \in G$,

$$g^x = \begin{bmatrix} g\theta_1 & & 0 \\ & \ddots & \\ * & & g\theta_r \end{bmatrix},$$

where the θ_i are irreducible representations of degrees n_i, and $n = n_1 + \ldots + n_r$. $K = \ker(g \longmapsto g\theta_1 \oplus \ldots \oplus g\theta_r)$

is a unitriangularizable group, nilpotent of class at most r. //

The next result is the one that is supposed to enable us to reduce from the imprimitive case to the primitive case.

2.2: Theorem. Let G be an imprimitive irreducible subgroup of GL(n,P) and let $\{Q_1, \ldots, Q_k\}$ be a complete system of imprimitivity for G in $P^{(n)}$. Set $H = \bigcap_{i=1}^{k} N_G(Q_i)$, $H_i = N_G(Q_i)$ and $\bar{H}_i = N_G(Q_i)\big|_{Q_i}$. Then $H \lhd G$, G/H is isomorphic to a transitive subgroup of S_k, the symmetric group of degree k, and H is isomorphic to a subgroup of $\bar{H}_1 \times \ldots \times \bar{H}_k$ (here "×" means external direct product). The groups $\bar{H}_i$ are primitive irreducible subgroups of GL(n/k,P). We also have that G is embedded in the permutational wreath product of H_1 by G/H, with G/H here considered as a permutation group of degree k. This embedding in turn embeds in GL(n,P). The new representation of G on $P^{(n)}$ thus obtained is that induced from $H_1 \leq G$: that is, $P^{(n)} \cong {Q_1}^G$, where the lefthand side is considered as a G-module via the new representation, and the Q_1 in the righthand side is considered as H_1-module in the natural way.

Proof: Let $g\theta$ be the permuation of $\{Q_1, \ldots, Q_k\}$ induced by $g \in G$, then θ is a homomorphism of G onto a subgroup of S_k which is transitive because G is irreducible, and clearly the kernel of θ is H.

Define a map μ from H into $\bar{H}_1 \times \ldots \times \bar{H}_k$ by, for $g \in H$,

$$g\mu = (g|_{Q_1}, \ldots, g|_{Q_k}).$$

For $g,h \in H$, it is not hard to see that $(gh)|_{Q_i} = g|_{Q_i}.h|_{Q_i}$, so μ is a homomorphism, and is clearly monic.

We next show that $\bar{H}_i$ is primitive and irreducible. For notational convenience, we only show this for i=1.

Irreducibility: suppose that R_1 is a proper non-trivial $\bar{H}_1$-invariant subspace of Q_1. Let $1=g_1, \ldots, g_k$ be a full set of coset representatives of H_1 in G - it is easy to verify that $[G:H_i] = k$ for all i - and observe that since G is irreducible,

$$P^{(n)} = Q_1g_1 \oplus \ldots \oplus Q_1g_k;$$

by renumbering the g_i if necessary, we can assume that $Q_1g_i = Q_i$. Consider the subspace R of $P^{(n)}$ defined by $R = R_1g_1 \oplus \ldots \oplus R_1g_k$ - clearly R is a proper non-trivial G-invariant subspace of $P^{(n)}$, contradicting the assumed irreducibility of G. So the subspace R_1 cannot exist and $\bar{H}_1$ is irreducible.

Primitivity: suppose $\{Q_{11}, \ldots, Q_{1\ell}\}$ is a system of imprimitivity for $\bar{H}_1$ in Q_1. We shall show that $\{Q_{ij} = Q_{1j}g_i : i=1,\ldots,k;\ j=1,\ldots,\ell\}$ is a system of imprimitivity for G, contradicting the minimality of $\{Q_1, \ldots, Q_k\}$, unless $\ell = 1$, so establishing the primitivity of $\bar{H}_1$.

For each $g \in G$, $Q_{ij}g = Q_{1j}g_ig$

$$= Q_{1j}h_1g_{i\alpha} \text{ (some } h_1 \in H_1,\ \alpha \in S_k)$$

$$= Q_{1,j\beta}g_{i\alpha} \text{ (some } \beta \in S_\ell)$$

$$= Q_{i\alpha,j\beta}.$$

So $\{Q_{ij}\}$ is a system of imprimitivity for G, as claimed.

Since elements of G permute the cosets of H_1, suitably ordered, in the same way as they permute the subspaces Q_i, G is embedded in the permutational wreath product of H_1 by $G\theta$, where θ is as in the first line of this proof, via the Frobenius embedding. Now H_1 has a representation on $P^{(n/k)}$ (namely $h \mapsto h|_{Q_1}$); it follows that H_1 Wr $G\theta$ has a representation on $P^{(n)}$, in which each copy of H_1 acts on a copy of $P^{(n/k)}$, and the $g\theta$'s permute the copies of $P^{(n/k)}$ in the same way that they permute the copies of H_1 in the wreath product. According to Kovacs 1967, this representation is (isomorphic to) that induced from the representation of H_1 referred to above. But, by Curtis and Reiner 1962, (50.2), the representation induced from that of H_1 is equivalent to the original faithful irreducible imprimitive representation of G on $P^{(n)}$. That is, $P^{(n)} = Q_1{}^G$ in the sense of the statement of the theorem. //

2.3: Corollary. If G is a maximal soluble irreducible imprimitive subgroup of GL(n,P), the above result can be sharpened by adding: $G = \bar{H}_1$ Wr $G\theta$, and $\bar{H}_1$ is a maximal soluble primitive irreducible subgroup of GL(n/k,P). The wreath product above is intended in the obvious sense - $G\theta$ permutes copies of $\bar{H}_1$ in the same way as it permuted copies of H_1 in 2.2.

Proof: $\bar{H}_1$ Wr $G\theta$ is embedded in GL(n,P), and contains (a conjugate of) G. Equality follows from maximality.

The reason for the maximality and solubility of the $\bar{H}_i$ is clear. //

2.4: Lemma. Let $H \rhd L$ be subgroups of $GL(n,P)$ such that $[H,L] \leq P^x.I_n$, and put $K = C_H(L)$. Then $[H:K] \leq n^2$, $H^n \leq K$, and the elements of any transversal from K to H are linearly independent over P.

Proof: Let $\{a_1, \ldots, a_t\}$ be any finite subset of a transversal from K to H, and suppose that it is linearly dependent over P. By renumbering if necessary, we can assume that

$$\lambda_1 a_1 + \ldots + \lambda_s a_s = 0$$

is a nontrivial linear relation of minimal length $s \geq 2$. In particular, for all i, $\lambda_i \neq 0$. Suppose that for each $x \in L$, $[a_1,x] = [a_2,x]$. Then

$$[a_1 a_2^{-1},x]^a = [a_1,x][a_2,x]^{-1} = 1,$$

so $[a_1 a_2^{-1},x] = 1$, and $a_1 a_2^{-1} \in K$. This contradicts the choice of the a_i, so there exists some $y \in L$ such that $[a_1,y] \neq [a_2,y]$. Since $[H,L] \leq P^x.I_n$, for each i, $[a_i,y] = \alpha_i I_n$ for some $\alpha_i \in P^x$, and $\alpha_1 \neq \alpha_2$.

Thus
$$0 = \alpha_1(\lambda_1 a_1 + \ldots + \lambda_s a_s) - (\lambda_1 a_1 + \ldots + \lambda_s a_s)^y$$
$$= \sum_2^s (\alpha_1 - \alpha_i)\lambda_i a_i$$

and this relation is nontrivial, since the coefficient of a_2 is nonzero. It is of length at most s-1: this contadicts the minimality of s. So $\{a_1, \ldots, a_t\}$ is linearly independent over P, whence $t \leq n^2$, and even $[H:K] \leq n^2$.

If $x \in H$, $y \in L$, then $xy = \lambda yx$ for some $\lambda \in P$. Thus $(\det x).(\det y) = \lambda^n(\det y).(\det x)$, which shows that $\lambda^n = 1$. Thus $x^n y = \lambda^n y x^n = y x^n$, and hence $x^n \in K$. That is, $H^n \leqslant K$. //

2.5: Definition. Symplectic groups. Let V be a vector space over P and $f: V \times V \to P$ a bilinear form on V. f is called an alternating form if for all $v \in V$, $f(v,v) = 0$, and non-degenerate if $f(v,V) = (0)$ implies that $v = 0$. It can easily be shown that

$$\{g \in GL(V): \forall\, u,v \in V \; f(ug,vg) = f(u,v)\}$$

is a subgroup of GL(V), for any bilinear form f. In the case where f is alternating, the above group is called the full symplectic group on V with respect to f. It can be shown (e.g. Huppert 1967, II.9.6) that a nondegenerate symplectic space, that is, a space V together with a non-degenerate alternating form, is always of even dimension - $\dim_P V = 2k$ for some k, and that the full symplectic group on V is determined up to isomorphism by the number k and the field P. In view of this, we are justified in denoting the full symplectic group on $P^{(2k)}$ by Sp(2k,P) (or Sp(2k,q) if P = GF(q)).

We also quote from Huppert 1967, II.9.13b the fact that the order of Sp(2k,p) is

$$p^{k^2}.(p^{2k} - 1)(p^{2k-2} - 1)\ldots(p^2 - 1).$$

The following is the theorem which provides information about the structure of primitive irreducible linear groups.

2.6: Theorem. Let G be a primitive irreducible subgroup of GL(n,P), and let F be a maximal Abelian normal subgroup of G. Put $V = C_G(F)$ and define A to be a subgroup of V maximal with respect to A/F being an Abelian normal subgroup of G/F. Then A is the Fitting subgroup of V, so is the unique subgroup of V maximal with respect to A/F being an Abelian normal subgroup of G/F, and

(i) F is a subgroup of the multiplicative group of a field K contained in P_n, and $\dim_P K$ divides n;

(ii) A/F is a direct product of elementary Abelian Sylow subgroups A_{p_i}/F, where $|A/F| = p_1^{2k_1} \ldots p_t^{2k_t} \leqslant r^2$, here $r = n/\dim_P K$. In fact, A is the central product of its subgroups A_{p_i} amalgamating F;

(iii) $V/C_V(A/F)$ is isomorphic to a subgroup of $Sp(2k_1,p_1) \times \ldots \times Sp(2k_t,p_t)$;

(iv) G/V is isomorphic to a subgroup of Gal(K;P), and so the index of V in G is at most $\dim_P K$;

(v) $C_V(A/F) = A \curlyvee_F C_V(A)$.

Proof: Part (i) is simply (0.6), together with the trivial relation $F \leqslant [F]^x$.

(a) Z(A) = F. $A \leqslant C_G(F)$, so $F \leqslant C_G(A)$, but also $F \leqslant A$, hence $F \leqslant A \cap C_G(A) = Z(A)$. In particular, A is nilpotent of class at most 2, so in view of 1.3,

$A \leqslant \mathrm{Fit}(V)$, and hence, by the maximality of A, $A = \mathrm{Fit}(V)$.

(b) Sylow subgroups of A/F are elementary Abelian.

Let A_p/F be a Sylow p-subgroup of A/F and suppose that it has exponent p^e, $e \geqslant 2$. Set $B = A^{p^{e-1}}$. Then B is characteristic in A_p, and A_p is normal in both A and G, so B is normal in G. Since, by (a), A is class 2 nilpotent, we have $[x,y]^{p^e} = [x^{p^e},y] = 1$ for all $x,y \in A_p$, because $x^{p^e} \in F$. Hence, for all $x,y \in A_p$,

$$[x^{p^{e-1}},y^{p^{e-1}}] = [x^{p^e},y^{p^{e-2}}] = 1 \text{ since}$$

$e - 2 \geqslant 0$. Thus B is Abelian, so contained in F. But this means that A_p/F has exponent p^{e-1}, contradiction.

(c) V is isomorphic to an irreducible subgroup of $GL(r,K)$, where $r = n/\dim_p K$, and $|A/F| = \dim_K [A] \leqslant r^2$.

(Here [A] denotes either the P-linear hull of A or the K-linear hull, which are identical in this instance.) The first part follows from (0.6(i)). The second part now follows from lemma 2.4, which says that $\dim_K [A] = |A/F| \leqslant r^2$, since as remarked above, the two available notions of linear hull are here equivalent.

(a), (b), and (c) together prove (ii), except for the assertion that $|A_{p_i}/F| = p_i^{2k_i}$, which will appear as a consequence of section (f).

(d) $Z(A_p) = F$ for all primes p.

$Z(A_p)$ is an Abelian normal subgroup of G containing F, so is equal to F by the latter's maximality property.

(e) Lemma A: If A/F has an element of order j, then so does F.

proof of lemma A: Let $a \in A$ be such that aF has order j. Because of the facts that A/F is finite and that $c^{-1}c' \in F$ implies $[a,c] = [a,c']$, it is true that $\{[a,c]: c \in A\}$ is a finite subgroup of F and hence of K^x. Now every finite subgroup of the multiplicative group of a field is cyclic, so $\{[a,c]: c \in A\}$ is a cyclic group, of order j', say. Thus $\forall c \in A$, $1 = [a,c]^{j'} = [a^{j'},c]$, so that aF has exponent j' - and j must divide j'. On the other hand, $[a,c]^{j} = [a^{j},c] = 1$, so j' divides j. So j = j', and $\{[a,c]: c \in A\}$ and a fortiori F contains an element of order j. //lemma A

Note for future use the fact that since all finite subgroups of multiplicative groups of fields are cyclic, F has exactly one cyclic subgroup of order $|aF|$.

(f) $V/C_V(A/F)$ is isomorphic to a subgroup of $Sp(2k_1,p_1) \times \ldots \times Sp(2k_t,p_t)$.

Since A_p/F, for p prime, is an elementary Abelian p-group, it can be regarded as a vector space over GF(p). It follows that $V/C_V(A_p/F)$ induces by conjugation a group of invertible linear transformations of A_p/F. (Linearity follows from $(ab)^h = a^h b^h$ and $(a^j)^h = (a^h)^j$ for $a,b \in A_p$, $h \in V$, and integers j.)

By lemma A, we can choose an element $e_p \in F$ with $|e_p| = p$ for each non-trivial Ap/F. By the proof of lemma A, for each pair $x,y \in A_p$, we can write

$[x,y] = e_p^u$ for some $u \in GF(p)$. We define a mapping $f: A_p/F \times A_p/F \to GF(p)$ by $(xF,yF)f = u$ and claim that f is a non-degenerate alternating form. It is easy to check that f is well-defined; that f is bilinear follows from the class 2 nilpotency of A_p; that f is alternating is obvious. Further,

$$(xF,A_p/F)f = (0) \text{ if \& only if } [x,A_p] = 1$$
$$\text{if \& only if } x \in Z(A_p) = F$$
$$\text{if \& only if } xF = 1_{A_p/F},$$

so f is non-degenerate as claimed. Consequently, A_p/F is a symplectic space of even dimension, 2k, say.

Now suppose that $(xF,yF)f = u$, in the usual notation. For all $h \in V = C_G(F)$,

$$[x^h,y^h] = [x,y]^h = (e_p^u)^h = e_p^u.$$

Hence $((xF)^h,(yF)^h)f = (xF,yF)f$ which means that each $h \in V$ induces a symplectic transformation of A_p/F. So $V/C_V(A_p/F)$ is isomorphic to a subgroup of $Sp(2k,p)$.

Clearly $C_V(A/F) = \bigcap_{i=1}^{t} C_V(A_{p_i}/F)$, so $V/C_V(A/F) \cong V/(\bigcap_i C_V(A_{p_i}/F))$, and by a well-known and straightforward result, the right-hand side of the last equation is isomorphic to a subgroup of $\prod_{i=1}^{t}(V/C_V(A_{p_i}/F))$. Hence $V/C_V(A/F)$ is isomorphic to a subgroup of $Sp(2k_1,p_1) \times \ldots \times Sp(2k_t,p_t)$ as claimed. This proves statement (iii) of the theorem.

(g) G/V is isomorphic to a subgroup of Gal(K:P); $|G/V| \leq \dim_P K$.

Certainly $G/C_G(F)$ is isomorphic to a subgroup of Aut(F), and, since G is a matrix group,

$$(f_1 + f_2)^g = f_1^g + f_2^g \quad \text{for } f_i \in F,\ g \in G,$$

so $G/C_G(F)$ induces isomorphisms on the linear hull of F - namely K - as well. This proves the first claim, the second follows from the first by Adamson 1964, theorem 14.2. This proves (iv).

(h) Lemma B: We can write the group A in the form $A = \mathrm{sgp}(a_1,b_1, \ldots ,a_\ell,b_\ell,F)$, where $\ell = \max_j k_j$, and $[a_i,b_i] = \epsilon_i$ is of order ν_i, as are a_iF and b_iF. The numbers ν_i have the property that ν_{i+1} divides ν_i, and are all squarefree. Also, the a_i's are permutable, the b_i's are permutable, and a_i and b_j are permutable for $i \neq j$.

proof of lemma B: Let ν_1 be largest among the orders of elements of A/F - that is, by (c), $\nu_1 = p_1 \cdots p_t$. By the proof of lemma A, A contains elements a_1,b_1 such that $[a_1,b_1] = \epsilon_1$ is of order ν_1. Because of the class 2 nilpotency of A, both a_1F and b_1F must have order ν_1. I claim that the group A can be written in the form $A = \mathrm{sgp}(a_1,b_1,A_1)$, where $A_1 = C_A(a_1,b_1)$. We prove this claim by showing that $[A:A_1] = \nu_1^2$.

Now there are exactly ν_1 elements in A conjugate to a_1. Specifically, the elements

$$a_1^{(b_1^j)} = \epsilon_1^j a_1, \quad j = 1,\ldots,\gamma_1$$

form a set of γ_1 elements conjugate in A to a_1, and the fact that, by the proof of lemma A, each $[a_1,x]$, $x \in A$, is a power of ϵ_1, entails that there can be no more than γ_1 such conjugates of a_1. Similarly, b_1 has γ_1 conjugates. Thus

$$[A:C_A(\{a_1,b_1\})] = [A:C_A(a_1)][C_A(a_1):C_A(a_1,b_1)] \leqslant \gamma_1^2.$$

On the other hand, the γ_1^2 elements of the form $a_1^{\alpha_1}b_1^{\beta_1}$ all belong to distinct cosets of A_1 in A, since $[a_1^{\alpha_1}b_1^{\beta_1},b_1] = \epsilon_1^{\alpha_1}$ and $[a_1,a_1^{\alpha_1}b_1^{\beta_1}] = \epsilon_1^{\beta_1}$.

Since the crucial properties of A are inherited by its subgroups, and since A_1 is a proper subgroup of A unless $l = 0$, this proves the theorem by induction on the order of A/F. Note that the permutability of a_i's and b_j's and the other properties in the statement of the lemma are trivial consequences of the definition of A_1 and γ_1.

(j) $\underline{C_V(A/F) = C_V(A) \curlyvee_F A}$.

We know already that $A \cap C_V(A) = Z(A) = F$, and that $F \leqslant C_G(V)$, so that $F \leqslant Z(C_V(A))$. Since the centre of $C_V(A) = C_G(A)$ is an Abelian normal subgroup of G, the maximality of F yields that $F = Z(C_V(A))$. Also, of course, $[A,C_V(A)] = \{1\}$. It therefore remains only to show that A and $C_V(A)$ together generate $C_V(A/F)$.

Suppose $c \in C_V(A/F)$. Decompose A as in the preceding lemma (B), and observe since $[a_i,c] \in F$ and $c \in V = C_G(F)$, and A is nilpotent of class 2, we have $[a_i,c]^{\nu_i} = [a_i^{\nu_i},c] = 1$ and similarly $[c,b_i]^{\nu_i} = 1$.

Thus, by the uniqueness of the cyclic subgroup of F generated by ϵ_i,

$$[a_i,c] = \epsilon_i^{\beta_i} \quad \text{for some integer } \beta_i$$

$$[c,b_j] = \epsilon_j^{\alpha_j} \quad \text{for some integer } \alpha_j.$$

Set $a = a_1^{\alpha_1} b_1^{\beta_1} \ldots a_\ell^{\alpha_\ell} b_\ell^{\beta_\ell}$. A simple calculation shows that $[a_i,a] = \epsilon_i^{\beta_i}$, $[a,b_i] = \epsilon_i^{\alpha_i}$,

so that $[a_i,a] = [a_i,c]$ and $[a,b_i] = [c,b_i]$. Now when $[x,y] \in F$ and $x,y \in C_G(F)$, it is true that $[x^{-1},y] = [x,y]^{-1}$, and from this fact and the nilpotency class 2 of A we can deduce that

$$[a_i,a^{-1}c] = [a^{-1}c,b_i] = 1$$

for $i = 1,\ldots,\ell$, that is, $a^{-1}c \in C_V(A)$. But this means that $c = a.a^{-1}c$, with $a \in A$, $a^{-1}c \in C_V(A)$, so A and $C_V(A)$ generate $C_V(A/F)$ as claimed.

This proves (v), and so completes the proof of theorem 2.6. //

2.7: Corollary. If G is a group satisfying the hypotheses of 2.6, and H is a soluble characteristic subgroup of V, then

(1) $C_H(A) = H \cap F = Z(H)$; and

(2) $H/Z(H)$ is finite.

Before proving 2.7, we state a particular case of it:

2.8: Corollary. If, with notation as in 2.6, V is a soluble group, then $C_V(A) = F$, so $C_V(A/F) = A$, so V/A is isomorphic to a subgroup of $Sp(2k_1,p_1)x...xSp(2k_t,p_t)$ and G/F is finite.

Proof of 2.8: Take H=V in 2.7, then $C_V(A) = F$, so by (v) of 2.6, $C_V(A/F) = A$. (iii) of 2.6 and the finiteness of the symplectic groups involved and of G/V, A/F lead to the two remaining conclusions. //

Proof of 2.7: (1a) $C_H(A) = H \cap F$. Suppose not, then $C_H(A)/F \cap H$, being soluble, has a non-trivial characteristic Abelian subgroup - call it $L/F \cap H$, say. We have $L/F \cap H \trianglelefteq G/F \cap H$, and thus $L \trianglelefteq G$. I claim that LA/F is Abelian. For $L \subseteq H$ implies that

$$F \cap L = F \cap H \cap L = F \cap H,$$

so that $L/F \cap H = L/F \cap L \cong LF/F$ is Abelian. Therefore LFA/F is Abelian, and of course LFA = LA. Clearly $LA \trianglelefteq G$ and $LA \leqslant V$, so by the maximality property of A, A = LA and $L \subseteq A$. So $F \cap H \subset L \subseteq A$. Also $L \leqslant C_H(A)$, so $L \leqslant A \cap C_H(A)$ which is contained in $Z(A) = F$. Hence $L \leqslant F$,

and, of course, $L \subseteq H$. So we have

$$F \cap H \subset L \subseteq F \cap H.$$

This contradiction establishes (1a).

(1b) $\underline{H \cap F = Z(H)}$. $H \subseteq C_G(F)$, so $F \subseteq C_V(H)$, so $F \cap H \subseteq C_V(H) \cap H = Z(H)$. Conversely, $Z(H)$ is an Abelian normal subgroup of G, so that $Z(H).F$ is also an Abelian normal subgroup of G, in view of the fact that $F \subseteq C_V(H)$. By the maximality of F, as usual, $F = Z(H).F$, so $Z(H) \subseteq F \cap H$.

(2) To establish that $H/Z(H)$ is finite, we observe that $H/C_H(A/F)$ is finite, since it is part of the automorphism group of the finite group A/F; it therefore remains to show that $C_H(A/F)/F \cap H$ is finite, (in view of (1b)).

Because $H \subset V$, each $h \in C_H(A/F)$ induces a well-defined homomorphism ϕ_h of A/F into F, given by

$$aF \longmapsto [a,h].$$

Since A normalises H, $\text{im } \phi_h \subseteq H$, so in fact in $H \cap F$, and so $h \longmapsto \phi_h$ is a map of $C_H(A/F)$ into $\text{Hom}(A/F, F \cap H)$. It is not hard to see, using the definition of $C_H(A/F)$, that this map is a homomorphism and that $\ker(h \longmapsto \phi_h) = C_H(A) = F \cap H$ by (1a) above. Since A/F is a torsion group and is finitely generated, and $F \cap H$ is locally cyclic, $\text{Hom}(A/F, F \cap H)$ is finite. It follows that $C_H(A/F)/F \cap H$ is finite. //

The next result uses Zassenhaus's theorem that locally soluble linear groups are soluble to prove a parallel result relating to nilpotency in primitive irreducible linear groups. This is then used to prove a result promised in chapter 1, outlining a situation when the Hirsch-Plotkin radical is nilpotent. Zassenhaus's theorem can be derived from 2.8, in a fashion similar to the proof given in Suprunenko 1963, page 32 and preceding pages, but not briefly, so it will not be proved here. Another important result (used in the proof of Zassenhaus's theorem, in fact) which can be derived from 2.8 is the theorem of Mal'cev which says that a soluble linear group always has a triangularizable normal subgroup of finite index.

2.9: Corollary. Let G and V be as in the statement of 2.6, and let H be a locally nilpotent characteristic subgroup of V. Then H is nilpotent.

Proof: Since H is locally nilpotent, it is certainly locally soluble, so by Zassenhaus's theorem H is soluble. Thus, by 2.7, $H/Z(H)$ is finite, and so nilpotent. Thus H is nilpotent. //

2.10: Corollary. Let V be as in 2.6. Then the Hirsch-Plotkin radical of V, $\rho(V)$, is nilpotent, and so, by 1.3, $\rho(V)$ is nilpotent of class at most 2.

Proof: $\rho(V)$ is a characteristic subgroup of V, so by 2.9 is nilpotent.

For use in the next chapter, we also quote here some extra results obtained by Suprunenko for the case of a maximal soluble primitive irreducible subgroup of GL(n,P) - he obtains (in Suprunenko 1963) that, in the notation of 2.6, A/F has order exactly n^2/m^2, where $m = \dim_P K$. This result takes surprisingly long to prove.

3. Maximal Soluble Primitive Irreducible Subgroups of GL(2,P).

In this section, we apply results of Suprunenko 1963 to the special case of maximal soluble primitive irreducible subgroups G of GL(2,P). We obtain results giving slightly more information than Suprunenko did in his book (section 2.3 of Suprunenko 1963) - specifically, we find that such groups are often split extensions under slight conditions on the field P.

With notation as in 2.6 and the suceeding results, consider the normal series

$$G \trianglerighteq V \trianglerighteq A \trianglerighteq F,$$

we know that F is (by maximality of G) the whole multiplicative group of a field $K \subseteq P_2$ and that $\dim_P K$ divides the degree of G - namely 2; that is, $K = P$ or $\dim_P K = 2$. Further, by the result mentioned at the end of the previous chapter, A/F has order 4 in the former case and 1 in the latter case. Let us consider the latter case first.

Case where $\dim_P K = 2$. We have $V = A = F$ and G/V is of order 2 by the maximality of G. If gV is a generator of G/V, then g is a non-scalar matrix whose square lies in F.

Case where $\dim_P K = 1$. This time we have $F = P^x.I_2$ and $V = G$. G/A is isomorphic to a subgroup of $Sp(2,2) \cong S_3$, which is a soluble group, so by maximality of G, G/A is isomorphic to the whole of

$Sp(2,2) = GL(2,2)$. Also A/F is generated by two elements aF and bF which have the properties

$$|aF| = |bF| = |[a,b]| = 2.$$

We need a lemma:

3.1: Lemma. If c is a non-scalar 2x2 matrix over a field P of characteristic $\neq 2$, such that c^2 is a scalar matrix, then the characteristic polynomial of c is $x^2 + \det c$. If $-\det c$ has a square root in P, then c is conjugate in $GL(2,P)$ to

$$\pm \begin{bmatrix} (-\det c)^{\frac{1}{2}} & 0 \\ 0 & -(-\det c)^{\frac{1}{2}} \end{bmatrix}.$$

Otherwise, c is conjugate to

$$\begin{bmatrix} 0 & 1 \\ -\det c & 0 \end{bmatrix}.$$

Proof: The second part is, of course, just a straightforward application of the theory of companion matrices to the conclusion of the first part.

If we suppose that $c = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$, and calculate c^2, then the assumption that c^2 is a scalar matrix leads to the equations

$$p^2 = s^2, \quad q(p + s) = r(p + s) = 0.$$

If $p + s$ were nonzero, then we would have $p = s$ and $q = r = 0$, so that c would be scalar: a contradiction. Hence $p + s = 0$.

Thus $\det(c - x.I_2) = (p - x)(s - x) - qr$

$= \det c - (p + s)x + x^2$

$= x^2 + \det c,$

as claimed. //

The theorem stated below embodies what is proved in this chapter: it outlines the structure of maximal soluble primitive irreducible subgroups of GL(2,P), and specifies the structure fairly precisely in the case when the fields K and P are equal.

3.2: Theorem. Let G be a maximal soluble primitive irreducible subgroup of GL(2,P). Then either (i) G consists of the multiplicative group of an extension field K of P of degree 2 extended by a group of order 2 which acts on K as a field automorphism fixing P, or (ii) the characteristic of P is $\neq 2$, and G is conjugate in GL(2,P) to one of the two following groups:

(a) if the generators a,b below can both be chosen to be of order 4, then G is conjugate to

$$\mathrm{sgp}(a,b,g_1,h,P^x.I_2),$$

where $\mathrm{sgp}(a,b) \cong$ quaternions, $\mathrm{sgp}(a,b,P^x.I_2) = A$, and

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad b = \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix} \text{ and } \alpha^2 + \beta^2 + 1 = 0,$$

$$g_1 = \tfrac{1}{2}\begin{bmatrix} \alpha-\beta-1 & \alpha+\beta+1 \\ \alpha+\beta-1 & \beta-\alpha-1 \end{bmatrix}, \quad h = \begin{bmatrix} \alpha & \beta-1 \\ \beta+1 & -\alpha \end{bmatrix}$$

and if P contains a square root for -2, the extension of A by G/A splits; this being true also in case (b);

(b) in the contradictory case to (a), G is conjugate to $sgp(a,b,g_1,h,P^x.I_2)$, where this time $sgp(a,b)$ is the dihedral group of order 8, A is as before, and

$$a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$g_1 = \tfrac{1}{2}(i+1)\begin{bmatrix} -1 & i \\ 1 & i \end{bmatrix}, \quad h = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ with } i^2 = -1.$$

Proof: The $\dim_p K \neq 1$ case has already been handled, and we know various things about a,b - in particular, that they satisfy the condition of lemma 3.1.

(a) It is not hard to see that in this case, the generators a,b are of the second type indicated in lemma 3.1. For the moment, let us only assume that a is conjugate to (and so may be taken as equal to) $\begin{bmatrix} 0 & 1 \\ -\det a & 0 \end{bmatrix}$, and that, by the proof of 3.1, b is of the form $\begin{bmatrix} \alpha & \beta \\ \gamma & -\alpha \end{bmatrix}$, (noting that this form is invariant under conjugation.) We will show that these conditions imply the condition of (a), so that to prove (b), it would only be necessary to consider the case when a is of the first type indicated in lemma 3.1. Calculating, using the fact that $[a,b] = -I_2$ we find

$$\begin{bmatrix} \gamma^2+\delta\alpha^2 & \alpha(\delta\beta-\gamma) \\ -\delta\alpha(\gamma-\delta\beta) & \delta(\alpha^2+\delta\beta^2) \end{bmatrix} = -\delta(\beta\gamma+\alpha^2).I_2$$

where $\delta = \det a$.

Hence $\gamma^2 = \delta^2\beta^2$, $\gamma^2 = \delta\beta\gamma$, $\alpha(\delta\beta - \gamma) = 0$, and $\beta\gamma = \delta\beta^2$. ...(2)
In order that b be nonsingular, therefore, at least one of α, β must be nonzero, whence $\gamma = \delta\beta$, that is,

$$b = \begin{bmatrix} \alpha & \beta \\ \delta\beta & -\alpha \end{bmatrix}.$$

We now recall that G/A is isomorphic to GL(2,2), which is generated by the matrices $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. On referring to the proof of this isomorphism in chapter 2, we see that G is generated mod A by matrices g,h whose action on A is given by the formulae:

$$\left.\begin{aligned} g^{-1}ag &= \lambda b, \quad h^{-1}ah = \lambda' b \\ g^{-1}bg &= \mu ab, \quad h^{-1}bh = \mu' a \end{aligned}\right\} \quad ...(1)$$

where $\lambda, \mu, \lambda', \mu'$ are elements of P^x.

Squaring the equations (1) and equating the coefficients gives
$\det a/\det b = \lambda^2 = \lambda'^2$, $\mu^2 = 1/\det a$, $\mu'^2 = \det b/\det a$, so that det a and det b must have square roots in P.

Observing that for any matrix c, $\det(c/(\det c)^{\frac{1}{2}}) = 1$ when det c has a square root, we now assume without loss of generality that a and b both have determinant equal to 1. Thus $\delta = 1$, $\alpha^2 + \beta^2 + 1 = 0$, and

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad b = \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}$$

Furthermore, we now have $\lambda^2 = \lambda'^2 = \mu^2 = \mu'^2 = 1$, that is, each of $\lambda, \lambda', \mu, \mu'$ is ± 1.

For each of g,h we are now confronted with four sets of equations, depending on the values of the λ's and μ's. We designate the corresponding solutions as follows: g_{++}, g_{+-}, g_{-+}, g_{--}, h_{++}, h_{+-}, h_{-+}, h_{--}, where the first sign indicates the value of λ or λ', and the second the value of μ or μ'. Then simple calculations show that if we have solutions g_{++}, h_{++} then $g_{+-} = g_{++}.b$, $g_{--} = g_{++}.a$, $g_{-+} = g_{++}.ab$ and $\underset{\sim}{h_{+-}} = h_{++}^{-1}.a$, $h_{--} = a.h_{++}^{-1}.a$, $\underset{\sim}{h_{-+}} = a.h_{++}$ are solutions for the remaining sets of equations. We may therefore assume without loss of generality that $\lambda = \lambda' = \mu = \mu' = 1$, and forget the notation above.

We now substitute $a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}$ into equations (1) with $\lambda = \lambda' = \mu = \mu' = 1$, and, using the fact that $\alpha^2 + \beta^2 + 1 = 0$, solve. It turns out that h must be some scalar multiple of

$$\begin{bmatrix} \alpha & \beta - 1 \\ \beta + 1 & -\alpha \end{bmatrix}$$

and that either $\alpha\beta + \alpha + \beta = 0$ or g is a scalar multiple of $\frac{1}{2}\begin{bmatrix} \alpha - \beta - 1 & \alpha + \beta + 1 \\ \alpha + \beta + 1 & \beta - \alpha - 1 \end{bmatrix}$ the above scalar multiple being chosen (after much labour) so that $g^3 = I_2$. We must dispose of the case $\alpha\beta + \alpha + \beta = 0$.

Observe that the only other restriction placed on α,β is that $\alpha^2 + \beta^2 + 1 = 0$, which remains true when the transformations $\alpha \mapsto -\alpha$, $\beta \mapsto \beta$ and $\alpha \mapsto \alpha, \beta \mapsto -\beta$ are applied. Note that all of

$$\alpha\beta + \alpha + \beta = 0$$
$$(-\alpha)\beta + (-\alpha) + \beta = 0$$
$$\alpha(-\beta) + \alpha + (-\beta) = 0$$

cannot simultaneously be true in our case, because they together imply that $2\alpha = 0$, $2\beta = 0$, which is impossible, since char P $\neq 2$. Finally, calculate that conjugation by $\begin{bmatrix} \beta & \alpha \\ -\alpha & \beta \end{bmatrix}$ and $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ fixes a and takes b to $\begin{bmatrix} -\alpha & \beta \\ \beta & \alpha \end{bmatrix}$ and $\begin{bmatrix} \alpha & -\beta \\ -\beta & -\alpha \end{bmatrix}$ respectively, thus effectively accomplishing the transformations $\alpha \mapsto -\alpha, \beta \mapsto \beta$ and $\alpha \mapsto \alpha, \beta \mapsto -\beta$, again respectively. So we may assume that $\alpha\beta + \alpha + \beta \neq 0$.

It remains to juggle g,h so that the extension of A by G/A splits. By trial and error, it was found that if we put $g_1 = (g^{-1})^a$ and $h_1 = (-\frac{1}{2})^{\frac{1}{2}}h$, (here using the assumption that P contains a square root for -2), then $[g_1,h_1] = g_1$, $g_1^3 = I_2 = h_1^2$, and thus $\mathrm{sgp}(g_1,h_1) \cong S_3$; hence the extension splits.

(As indicated in the statement of the theorem, one calculates that $g_1 = \frac{1}{2}\begin{bmatrix} \alpha-\beta-1 & \alpha+\beta+1 \\ \alpha+\beta-1 & \beta-\alpha-1 \end{bmatrix}$.)

(b) The proof of this part is similar to that of (a), with numerical simplifications, so will be omitted.

This result attaches interest to fields which contain elements α, β such that $\alpha^2 + \beta^2 + 1 = 0$, and to fields which have square roots of -2. Clearly, algebraically closed fields of characteristic $\neq 2$ satisfy both conditions. Also, according to Herstein 1964, lemma 7.7, every finite field satisfies the first condition. Square roots of -2 are, of course, rarer in finite fields.

4. Tensor Product Decomposition of Primitive Irreducible Linear Groups.

We employ the notation of 2.4; G is a primitive irreducible subgroup of GL(n,P), F a maximal Abelian normal subgroup of G, V the centraliser of F in G, A/F maximal with respect to being an Abelian subgroup of V/F normal in G/F, and A_{p_i}/F is the Sylow p_i- subgroup of A/F.

In Suprunenko 1969 that author, using the extra assumption that G is also a maximal soluble subgroup of GL(n,P), shows that G is a tensor product of maximal soluble primitive irreducible subgroups of $GL(p_i^{k_i},P)$, $i = 1,\ldots,t$, where $n = p_1^{k_1}\ldots p_t^{k_t}$ (p_i prime and distinct). In this section, we will investigate this decomposition without the extra assumption. Two approaches will be used: first we try to build up an entirely group-theoretical decomposition inside V, then we obtain a description of V as a sort of subdirect tensor product of groups not necessarily contained in V.

Recall from 0.6 that A has a faithful irreducible representation in GL(r,K), and that V is also embedded in GL(r,K). We shall find it necessary later to assume that this irreducible representation of A is absolutely irreducible; the following example, pointed out by Dr M.F. Newman, shows that this absolute irreducibility condition does not always hold:

Example: We work in GL(4,Q), where Q is the field of rational numbers. Set

$$X = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \end{bmatrix}$$

$$Z = \tfrac{1}{2}\begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$$ and let G be the group generated by X,Y,Z.

It can be shown that G is primitive and irreducible, that F is the subgroup generated by X^2 and Y^2 (both are scalar matrices), that A is the subgroup generated by F together with X and X^Y.

Further, $sgp(X,X^Y)$ is the unique faithful irreducible representation of Q_8 over the rationals, so A is irreducible, but A is not absolutely irreducible, because it splits into two equivalent representations in GL(4,Q(i)). The appropriate change of basis matrix is

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -i & 0 & i & 0 \\ 0 & -i & 0 & i \end{bmatrix}.$$

In 4.6 and 4.14 we shall use without reference the following result:

4.0: Lemma. If $H_1,\dots,H_s$ are subgroups of a group H such that for each i,j:

$Z(H_i) = Z$, a fixed subgroup of H

$H_i \cap H_j = Z$ and $[H_i,H_j] = (1)$

the subgroups H_i generate H,

then $H = H_1 \curlyvee_Z \cdots \curlyvee_Z H_s$.

Proof: For each i, set $R_i = \mathrm{sgp}(H_j: j\neq i)$. We must prove that $[H_i,R_i] = (1)$ and $H_i \cap R_i = Z$. The first part is obvious, so we turn our attention to the second part.

If $x \in H_i \cap R_i$ then, by the first part, $x \in C_H(H_i)$. Since also $x \in H_i$, we have $x \in H_i \cap C_H(H_i) = Z(H_i) = Z$. Conversely, of course, $Z \subseteq H_i \cap R_i$, so $Z = H_i \cap R_i$ and we are finished. //

4.1 Lemma. Let H_1, H_2 be subgroups of a group H, such that $[H_1,H_2] = (1)$. Then $[C_HC_H(H_1),C_HC_H(H_2)] = (1)$; in particular, if H_1 is Abelian, then so is $C_HC_H(H_1)$.

Proof: $[H_1,H_2] = 1$ implies that $H_2 \subseteq C_H(H_1)$. It is easy to see that this entails that

$$C_HC_H(H_1) \subseteq C_H(H_1).$$

That is, $[C_HC_H(H_1),H_2] = (1)$. Repeating this process, we get $[C_HC_H(H_1),C_HC_H(H_2)] = (1)$. //

4.2 Notation. We will use the abbreviation C_{p_i} for the group $C_GC_G(A_{p_i}) = C_VC_V(A_{p_i})$. Easy manipulations lead to the relations $F \subseteq A_{p_i} \subseteq C_{p_i} \subseteq V$.

4.3 Corollary. $[C_p,C_q] = (1)$ for $p \neq q$.

Proof: If $p \neq q$, then $[A_p,A_q] = (1)$, hence, by 4.1, $[C_p,C_q] = (1)$. //

4.4 Lemma. If H_1, H_2 and H are as in 4.1, then

(i) $C_H(H_1) \cap C_H(H_2) = C_H(\mathrm{sgp}(H_1,H_2))$

(ii) $\mathrm{sgp}(C_H(H_1),C_H(H_2)) \subseteq C_H(H_1 \cap H_2)$.

Proof: Trivial manipulations. //

4.5 Proposition. $C_GC_G(F) = F$, and $p \neq q$ implies $C_p \cap C_q = F \subseteq Z(C_p)$.

Proof: By 4.1, $C_GC_G(F)$ is Abelian; certainly it is a normal subgroup of G. Also, clearly $F \subseteq C_GC_G(F)$. But F is a maximal Abelian normal subgroup of G so $F = C_GC_G(F)$. By 4.4,

$$C_p \cap C_q \leq C_G C_G(A_p \cap A_q)$$
$$\leq C_G C_G(F) = F.$$

Finally $F \subseteq Z(V)$ and $F \subseteq C_p \subseteq V$, so $F \subseteq Z(C_p)$. //

4.6: Corollary. The groups C_{p_i}, $i = 1,\ldots t$ generate their central product amalgamating F:

$$\mathrm{sgp}(C_{p_1},\ldots,C_{p_t}) = C_{p_1} \curlyvee_F \cdots \curlyvee_F C_{p_t}.$$

//

4.7: Lemma. $C_G(A_p/F) = C_G(A_p) \curlyvee_F A_p$.

Proof: The only non-trivial part is to show that A_p and $C_G(A_p)$ together generate all of $C_G(A_p/F)$. As usual, we can decompose A_p to obtain

$$A_p = \mathrm{sgp}(a_1,b_1,\ldots,a_k,b_k,F)$$

where each a_jF, each b_jF is of order p;

$$[a_j,b_j] = \varepsilon_j, \quad |\varepsilon_j| = p, \quad \varepsilon_j \in F,$$ while all other pairs of a's and b's commute. Take any element c of $C_G(A_p/F)$, observe that for each i, j,

$$[a_i,c] \in F \text{ and } [c,b_j] \in F$$

and $[a_i,c]^p = [a_i^p,c] = 1 = [c,b_j]^p$, so that we can write $[a_i,c] = \varepsilon_i^{\beta_i}$, $[c,b_j] = \varepsilon_j^{\alpha_j}$ and set

$$a = a_1^{\alpha_1} b_1^{\beta_1} \cdots a_k^{\alpha_k} b_k^{\beta_k}.$$

Calculations now show $[a_i,a] = [a_i,c]$ for each i

and $[a,b_j] = [c,b_j]$ for each j

and consequently $[a_i,a^{-1}c] = [a^{-1}c,b_j] = 1$.

That is, $a^{-1}c \in C_G(A_p)$ and

$$c = a.a^{-1}c \in \mathrm{sgp}(A_p,C_G(A_p)) \quad //$$

4.8: Corollary. $C_{p_i} \cap C_G(A_{p_i}/F) = A_{p_i}$.

Proof: $C_G C_G(A_{p_i}) \cap (C_G(A_{p_i}).A_{p_i}) = Z(C_G(A_{p_i})).A_{p_i}$
$= F.A_{p_i}$
$= A_{p_i}$. //

4.9: Lemma. If $F \subseteq B_i \subseteq A_i \subseteq H$ and $F \subseteq Z(A_i)$ for all i, then $\Upsilon_i A_i/\Upsilon_i B_i \cong \oplus_i (A_i/B_i)$.

Proof: Certainly

$$\oplus_i A_i/\oplus_i B_i \cong \oplus_i (A_i/B_i).$$

In general, if $C \trianglelefteq D$ and θ is a homomorphism defined on D, then $\ker\theta \subseteq C$ entails that $D/C \cong D\theta/C\theta$: this is one of the Isomorphism Theorems. By its definition, $\Upsilon_i A_i$ is a homomorphic image of $\oplus_i A_i$, and since $F \subseteq B_i$, the kernel of the defining homomorphism is contained in $\oplus_i B_i$. //

4.10: Theorem. $(\Upsilon_i C_{p_i})/A$ is isomorphic to a direct product of symplectic groups isomorphic to the C_{p_i}/A_{p_i}.

Proof: In view of 4.9, it is only necessary to show that the C_{p_i}/A_{p_i} are isomorphic to symplectic groups. Examination of the proof of 2.4 shows that $C_{p_i}.C_G(A_{p_i}/F)/C_G(A_{p_i}/F)$ induces a group of symplectic transformations of A_{p_i}/F. Now

$$C_{p_i}.C_G(A_{p_i}/F)/C_G(A_{p_i}/F) \cong C_{p_i}/(C_{p_i} \cap C_G(A_{p_i}/F))$$
$$\cong C_{p_i}/A_{p_i} \text{ by 4.8. //}$$

The following discussion connects central products and tensor products.

Suppose that B_1, B_2 are normal subgroups of G contained in V and intersecting in F, and that U_i is the faithful irreducible B_i-module provided by 0.6(i) for $i = 1,2$. Observe that since $K = [F]$ is contained in the P-linear hull of B_i, the proof of 0.6(i) can be extended to show that if for some fixed $b_i \in B_i$ and all $u_i \in U_i$ $u_i b_i = k u_i$ for fixed $k \in K$, then $b_i = k$.

Construct $U_1 \otimes_K U_2$. I claim that this is a $B_1 \times B_2$ -module with action given by

$$(u_1 \otimes u_2)(b_1, b_2) = u_1 b_1 \otimes u_2 b_2.$$

To see that this action is well-defined, we must show that if $\sum_{j=1}^{n} v_{j1} \otimes v_{j2} = u_1 \otimes u_2$, (*) then $\sum_{j=1}^{n} v_{j1} b_1 \otimes v_{j2} b_2 = u_1 b_1 \otimes u_2 b_2$.

Fortunately, since U_1, U_2 are vector spaces over the field K, (*) implies that $n = 1$ and $v_{11} = k u_1$, $v_{12} = k^{-1} u_2$ for some $k \in K$, and then, since $B_i \subseteq V$,

$$(k u_1) b_1 \otimes (k^{-1} u_2) b_2 = u_1 b_1 \otimes u_2 b_2,$$

as required.

Now suppose that $(b_1, b_2) \in B_1 \times B_2$ induces the identity on $U_1 \otimes U_2$. An argument similar to that above yields that there exists $k \in K$ such that $\forall u_1 \in U_1$ $u_1 b_1 = k u_1$ and $\forall u_2 \in U_2$ $u_2 b_2 = k^{-1} u_2$. The initial observation now implies that $b_1 = k$ and $b_2 = k^{-1}$ (and so, in particular, $k \in F$). By the

definition of $B_1 \curlyvee_f B_2$ and the above remarks, $U_1 \otimes_k U_2$ is a faithful $B_1 \curlyvee_f B_2$ -module under the natural action. That is, " $b_1 \curlyvee b_2 = b_1 \otimes b_2$ ".

4.11: Corollary. $sgp(C_{p_i}, i = 1,\ldots,t)$ is the tensor product of its subgroups C_{p_i}.

Proof: Above remarks and 4.6. //

It would be preferable to show next that $sgp(C_{p_i}, i=1,\ldots,t) = V$, at least in the case when A is an absolutely irreducible subgroup of GL(r,K), but I cannot do this; the difficulty seems to arise from the lack of Suprunenko's maximality condition. So instead, we move on to the second approach mentioned at the beginning of this section.

4.12: Proposition. If A is absolutely irreducible as a subgroup of GL(r,K), then each $x \in V$ may be written as a product

$$x = x_1 x_2 \ldots x_t,$$

where x_i is an invertible element of $C_{[A_{p_i}]} C_V(A_{p_i})$.

Proof: Remembering that each $A_{p_i} \trianglelefteq G$, we have by 0.6 that $[A_{p_i}]$ is a simple algebra. Our element x of V induces an algebra automorphism of $[A_{p_i}]$ since distributivity of matrix multiplication entails that $x^{-1}(a + b)x = x^{-1}ax + x^{-1}bx$ for matrices a,b. So, by the Noether-Skolem theorem (Herstein 1968, theorem 4.3.1), there exists x_i in $[A_{p_i}]$ such that x_i is

invertible and, for all $a \in A_{p_i}$, $x_i^{-1} a x_i = x^{-1} a x$.

Consider $y = x^{-1}(x_1 \ldots x_t)$. Clearly $y \in C_{V.[A]}(A)$. Now V and [A] are embedded in K_r, and the absolute irreducibility of A means that $C_{K_r}(A) = K$ (see Huppert 1967, V.LL.LO). Thus $y \in K$ and we may write $x = x_1 \ldots x_t$.

Finally, it is easy to see that

$$[A_{p_i}] \subseteq C_{[A_{p_i}]} C_V(A_{p_i}). \qquad //$$

Motivated by the last line of the above proof, we invent the following notation:

4.13: Notation. $\mathcal{C}_{p_i}$ denotes the group generated by the nonzero elements of K and the matrices x_i as x ranges over V.

Calculations differing in no essential respect from those in 4.1, 4.3, 4.4, 4.5 show that if $p \neq q$, then $[\mathcal{C}_p, \mathcal{C}_q] = (1)$ and $\mathcal{C}_p \cap \mathcal{C}_q = K^x \subseteq Z(\mathcal{C}_p)$. Thus, once again the $\mathcal{C}_{p_i}$ generate their central product. So

4.14: Theorem. V is isomorphic to a subgroup of $\mathcal{C}_{p_1} Y_{K^x} \ldots Y_{K^x} \mathcal{C}_{p_t}$.

There remain some odds and ends to attend to. For instance, one could remark that the $\mathcal{C}_{p_i}$ clearly induce a symplectic action on A_{p_i}/F. AAless trivial question is: how well-determined are the x_i? To answer this, we refer to Lemma 3 of Suprunenko 1969.

It is proved there that the absolute irreducibility of A entails that of the A_{p_i} : that is, A_{p_i} is an absolutely irreducible subgroup of $GL(p_i^{k_i},K)$, where $r = p_1^{k_1}...p_t^{k_t}$ is the prime decomposition of r. Hence $C_{K_{p_i^{k_i}}}(A_{p_i}) = K$ as before with A. If there exist x_i and x_i' in $[A_{p_i}]$ such that for all $a \in A_{p_i}$,

$$x_i^{-1}ax_i = (x_i')^{-1}ax_i' \text{ , then clearly}$$

$x_i^{-1}x_i' \in C_{[A_{p_i}]}(A_{p_i}) = K$ by the remark above.
So x determines x_i up to a factor from K.

To link the section with what Suprunenko 1969 proved, the maximal soluble primitive irreducible subgroup G of GL(n,P), P algebraically closed, must be equal to the whole of $\bar{C}_{p_1}...\bar{C}_{p_t}$ by virtue of the maximality of G and the fact that the $\bar{C}_{p_i}$ are clearly soluble.

References.

I.T. Adamson, 1964; Introduction to Field Theory, Oliver and Boyd, Edinburgh.

C.W. Curtis and Reiner, I., 1962; Representation Theory of Finite Groups and Associative Algebras, Interscience, New York.

I.N. Herstein, 1964; Topics in Algebra, Blaisdell, Waltham, Mass.

I.N. Herstein, 1968; Noncommutative Rings, Mathematical Association of America.

B. Huppert, 1967; Endliche Gruppen, Springer, Berlin.

D.A. Suprunenko, 1963; Soluble and Nilpotent Linear Groups, American Mathematical Society Translations of Mathematical Monographs.

D.A. Suprunenko, 1969; On the theory of soluble linear groups, Sibirskiĭ Matematicheskiĭ Žurnal, volume 10, pages 1161-1172.

B.A. Wehrfritz; Infinite Linear Groups, Queen Mary College, London.

L. Kovacs, 1967; Three embedding theorems, seminar notes taken at A.N.U., Canberra.